PATENTS
Attorney Docket No. SMY-219.01
P4421

IN THE CLAIMS:

1. (Currently Amended) A method of operation at a file server, the method comprising:

~~accessing~~ storing ~~at said file server~~ (i) information encrypted with a first encryption key and (ii) ~~an entry from~~ an access control list usable by said file server to control access to said encrypted information, said access control list including an entry ~~being~~ that includes ~~associated with said encrypted information and~~ an identifier for a client authorized to at least read ~~and modify~~ said encrypted information~~, wherein said entry comprises~~ and a first decryption key encrypted with a second encryption key, ~~and~~ wherein said first decryption key is usable to decrypt said encrypted information, and wherein said second encryption key is associated with a second decryption key that is usable to decrypt said encrypted first decryption key and that is accessible to said client, and[[.]]

in response to a request from said client, transmitting to said client said encrypted information and said entry.

2-3. (Cancelled)

4. (Currently Amended) The method of claim 1 wherein ~~said~~ transmitting ~~step~~ comprises ~~the step of~~ transmitting to said ~~requesting~~ client said access control list.

5. (Original) The method of claim 1 wherein said first encryption key and said first decryption key are symmetric.

6. (Original) The method of claim 1 wherein said first encryption key comprises one of a public key and a private key of a first public/private key pair and said first decryption key comprises the other of said public key and said private key of said first public/private key pair.

7. (Currently Amended) The method of claim ~~2~~ 1 wherein ~~said step of storing said entry on said file server includes the step of storing in association with~~ said ~~entry~~ identifier includes one of an unecrypted identifier and an encrypted identifier ~~associated with said client~~.

8. (Currently Amended) The method of claim ~~2~~ 1 wherein ~~said step of storing said entry on said file server comprises the step of storing an access control list, wherein said entry comprises one entry of a plurality of entries within said access control list, and~~ said entry includes said first decryption key combined with a check value to form a data stream, wherein said data stream is encrypted with ~~a~~ said second encryption key ~~associated with said client~~; and

~~said~~ transmitting ~~step~~ comprises ~~the step of~~ transmitting to said ~~requesting~~ client said encrypted information and said access control list.

9. (Original) The method of claim 8 wherein said check value comprises a value known to said client.

10. (Currently Amended) The method of claim 8 wherein said check value comprises ~~an identifier associated with~~ said client identifier.

a1 11. (Cancelled)

12. (Currently Amended) The method of claim 8 wherein said check value ~~identifier~~ comprises a group identifier that identifies a group of which said client is a member.

13. (Currently Amended) A method for securely storing information on a file server and distributing the stored information, said method comprising:

encrypting information at one of a plurality of clients in communication with said file server, said information being encrypted with a first encryption key having an associated first decryption key that is usable to decrypt said encrypted information;

encrypting said first decryption key with a second encryption key for each of said plurality of clients authorized to at least read ~~and modify~~ said information, wherein each respective one of said second encryption keys has a corresponding second decryption key that is usable to decrypt said respective encrypted first decryption key and that is retained by the respective one of said plurality of clients;

storing said encrypted information on said file server and storing on said file server said encrypted first decryption keys as a plurality of entries within an access control list, wherein each one of said entries is associated with one of said plurality of clients;

forwarding to at least a selected one of said plurality of clients said encrypted information and at least one of said entries in response to a request received at said file server from said selected one of said plurality of clients;

decrypting said encrypted first decryption key contained in said at least one of said entries utilizing the second decryption key corresponding to the second encryption key for the respective entry; and

decrypting said encrypted information using said first decryption key to obtain said information.

14. (Cancelled)

15. (Currently Amended) The method of claim ~~14~~ 13 wherein said request includes a client identifier associated with said selected one of said plurality of clients, said entries each include a client identifier associated with one of said plurality of clients, and wherein ~~said~~ forwarding ~~step~~ includes ~~the step of~~ forwarding to at least said selected one of said plurality of clients the ~~said~~ entry including the client identifier that is associated with the client identifier contained within said request.

16. (Currently Amended) The method of claim 13 wherein ~~said~~ forwarding ~~step~~ comprises ~~the step of~~ forwarding to said selected one of said plurality of clients said encrypted information and said access control list.

17. (Currently Amended) The method of claim ~~17~~ 13 wherein said first encryption and decryption keys are symmetric.

18. (Original) The method of claim 13 wherein said second encryption and decryption keys are symmetric.

19. (Original) The method of claim 13 wherein said first encryption key comprises one of a public key and a private key of a first public/private key pair and the first decryption key comprises the other of said public key and said private key of said first public/private key pair.

20. (Currently Amended) A method for storing information securely on a file server for access by members of a group, said method comprising ~~the steps of~~:

identifying the members of said group, wherein said group has a group identifier,

encrypting information with a first encryption key having an associated first decryption key that is usable to decrypt said encrypted information;

encrypting said first decryption key with a group encryption key having an associated group decryption key for decrypting data encrypted with said group encryption key; ~~and~~

storing said encrypted information on said file server and storing said encrypted first decryption key on said file server within an access control list associated with said encrypted information and containing, at least at some times, a plurality of encrypted first decryption keys, and

in response to a request received at said file server from one of said members of said group, forwarding to said one of said members of said group said encrypted information and at least said first decryption key encrypted with said group encryption key.

21. (Currently Amended) A method for accessing information securely stored on a file server for access by members of a group, said method comprising:

identifying the members of said group, wherein said group has a group identifier,

encrypting information with a first encryption key having an associated first decryption key that is usable to decrypt said encrypted information;

encrypting said first decryption key with a group encryption key having an associated group decryption key for decrypting data encrypted with said group encryption key;

storing said encrypted information on said file server and storing said encrypted first decryption key on said file server within an access control list associated with said encrypted information and containing, at least at some times, a plurality of encrypted first decryption keys.

in response to a request received at said file server from one of said members of said group, forwarding to said one of said members of said group said encrypted information and at least said encrypted first decryption key encrypted with said group encryption key;

in a first decrypting ~~step~~, decrypting said encrypted first decryption key with said group decryption key to obtain said first decryption key; and

in a second decrypting ~~step~~, decrypting said encrypted information using said first decryption key to obtain said information.

22. (Currently Amended) The method of claim 21 wherein said method further includes ~~the step of~~ distributing said group decryption key to said members of said group and said first decrypting ~~step~~ comprises ~~the step of~~ decrypting the encrypted first decryption key by said one of said members of said group using the distributed group decryption key.

a1

23. (Currently Amended) The method of claim 21 wherein said first decrypting ~~step~~ comprises ~~the steps of~~:

forwarding said encrypted first decryption key to a group server associated with said group identifier;

decrypting said encrypted first decryption key at said group server using said group decryption key; and

forwarding said first decryption key to said one of said group members.

24. (Currently Amended) The method of claim 23 wherein ~~said step of~~ forwarding said first decryption key to said one of said group members comprises ~~the step of~~ forwarding the first decryption key to said one of said group members over a secure channel.

25. (Original) The method of claim 24 wherein said secure channel is a physically secure channel.

26. (Currently Amended) The method of claim 24 wherein said secure channel comprises a non-secure communications path and ~~said step of~~ forwarding the first decryption key to said one of said group members over a secure channel comprises ~~the steps of~~:

encrypting said first decryption key with a third encryption key having an associated third decryption key known to said one of said group members;

forwarding to said one of said group members said encrypted first decryption key encrypted with said third encryption key; and

decrypting by said one of said group members, said encrypted first decryption key encrypted with said third encryption key using said third decryption key.

27. (Original) The method of claim 26 wherein said third encryption key comprises a public key of a member public/private key pair and wherein said third decryption key comprises the member private key of said member public/private key pair.

28. (Original) The method of claim 26 wherein said third encryption and decryption keys are symmetric.

29. (Original) The method of claim 21 wherein said first encryption and decryption keys are symmetric.

30. (Original) The method of claim 21 wherein said first encryption key comprises one of a public key and a private key of a first public/private key pair and the first decryption key comprises the other of said public key and said private key of said first public/private key pair.

31. (Currently Amended) A method for accessing information stored securely on a file server, the method comprising:

forwarding to said file server a request for information from a client;

in response to said request, receiving from said file server said information encrypted with a first encryption key having an associated first decryption key that is usable to decrypt said encrypted information and at least one access control list entry associated with a client authorized to at least read ~~and modify~~ said information, said received at least one entry including said first decryption key encrypted with a second encryption key having an associated second decryption key that is usable to decrypt said encrypted first decryption key and that is accessible to said client;

decrypting said encrypted first decryption key using said second decryption key to obtain said first decryption key; and

decrypting said encrypted information using said first decryption key.

32. (Original) The method of claim 31 wherein said first encryption and decryption keys are symmetric.

33. (Original) The method of claim 31 wherein said first encryption key comprises one of a public key and a private key of a first public/private key pair and the first decryption key comprises the other of said public key and said private key of said first public/private key pair.

34. (Original) The method of claim 31 wherein said second encryption key comprises a public key of a member public/private key pair and said second decryption key comprises the private key of said member public/private key pair.

35. (Currently Amended) A computer program product including a computer readable medium, said computer readable medium having a file server computer program stored thereon, said file server computer program for execution in a computer and comprising:

program code for storing on said file server information encrypted with a first encryption key having a corresponding first decryption key that is usable to decrypt said encrypted information;

program code for storing on said file server an access control list, said access control list including at least one entry, said at least one entry including said first decryption key encrypted with a second encryption key associated with one of a plurality of clients authorized to at least read ~~and modify~~ said information and having access to a second decryption key associated with said second encryption key and usable to decrypt said encrypted first decryption key; and

program code for transmitting to said one of said plurality of clients said encrypted information and said at least one entry.

36. (Currently Amended) A computer data signal, said computer data signal including a computer program for use in accessing encrypted information stored on a file server, said computer program comprising:

program code for storing on said file server information encrypted with a first encryption key having a corresponding first decryption key that is usable to decrypt said encrypted information;

program code for storing on said file server an access control list, said access control list including at least one entry, said at least one entry including said first decryption key encrypted with a second encryption key associated with one of a plurality of clients authorized to at least read ~~and modify~~ said information and having access to a second decryption key associated with said second encryption key and usable to decrypt said encrypted first decryption key; and

program code for transmitting to said one of said plurality of clients said encrypted information and said at least one entry.

37. (Currently Amended) Apparatus for accessing encrypted data stored on a file server, the apparatus comprising:

means for storing on said file server information encrypted with a first encryption key having a corresponding first decryption key that is usable to decrypt said encrypted information;

means for storing on said file server an access control list, said access control list including at least one entry, said at least one entry including said first decryption key encrypted with a second encryption key associated with one of a plurality of clients authorized to at least read ~~and modify~~ said information and having access to a second decryption key associated with said second encryption key that is usable to decrypt said encrypted first decryption key; and

program code for transmitting to said one of said plurality of clients said encrypted information and said at least one entry.